The Essential WordPress Security Checklist

Account & User Security

Status	Security Step	Action/Notes
☐	**Use a Strong, Unique Password**	Use a password manager to generate a complex password (12+ characters, mixed case, symbols).
☐	**Enable Two-Factor Authentication (2FA)**	Install a plugin (e.g., WP 2FA, Google Authenticator) to require a code from your phone upon login.
☐	**Change the Default "admin" Username**	If you still have a user named "admin" or "administrator," create a new Admin user with a unique name, log in as the new user, and delete the old one.
☐	**Limit Login Attempts**	Install a plugin (e.g., Limit Login Attempts Reloaded) to block users after a specified number of failed login attempts (prevents brute-force attacks).
☐	**Review User Roles**	Ensure all users have the absolute minimum permissions they need (Principle of Least Privilege). Downgrade unnecessary Administrator accounts.

Core, Theme, & Plugin Protection

Status	Security Step	Action/Notes
☐	**Update Everything Regularly**	Keep the WordPress **Core**, all **Themes**, and all **Plugins** updated to their latest versions. *This is your #1 defense.*
☐	**Remove Unused Themes and Plugins**	Delete any plugins or themes that are not active or in use. They are potential security backdoors.
☐	**Install a Reputable Security Plugin**	Install a comprehensive security solution (e.g., Wordfence, Sucuri, iThemes Security) for firewall and malware scanning.

☐	**Enforce HTTPS (SSL Certificate)**	Ensure your entire site loads using https:// (look for the padlock in the browser bar).
☐	**Disable File Editing in WordPress**	Prevent unauthorized parties from modifying critical files by disabling the built-in file editor. Add define('DISALLOW_FILE_EDIT', true); to your wp-config.php file.

Server & Database Hardening

Status	Security Step	Action/Notes
☐	**Configure Regular Backups**	Set up an automated backup system (e.g., UpdraftPlus) to store both your files and database **offsite** (e.g., Dropbox, Google Drive).
☐	**Change the WordPress Database Prefix**	Change the default wp_ database prefix to a random unique string (if done on a *new* installation). This mitigates SQL injection risks.
☐	**Disable XML-RPC (If not needed)**	If you don't use the Jetpack app, the block editor, or remote publishing, disable XML-RPC to close a common brute-force vector.
☐	**Choose a Secure Web Host**	Verify that your hosting provider offers server-level security features like firewalls (WAF), monitoring, and resource isolation.

Recommended WordPress Apps Plugins

Tool / App	Category	Key Security Role
LastPass	Password Manager	Generates and securely stores unique, complex passwords for all your accounts, including your WordPress Master Password.
Secure PassKeys	Authentication	A modern, more secure alternative to passwords, relying on cryptography and biometric verification to log in (great for core login security).

WP 2FA	Login Protection	Enforces Two-Factor Authentication (2FA) for your WordPress site, ensuring that a compromised password alone is not enough to gain access.
Sucuri Security	Active Security & Monitoring	Provides malware scanning, file integrity monitoring, security hardening (e.g., disable file editing), and post-hack recovery tools.
UpdraftPlus	Backup & Recovery	The leading backup plugin, allowing you to easily schedule, store, and **restore** your entire site (files and database) offsite in case of a breach.
WP Mail SMTP	Reliability & Monitoring	Fixes email deliverability issues, ensuring that critical security alerts (e.g., from Sucuri or WP 2FA) are reliably sent and received.
Site Kit by Google	Diagnostics & Alerts	Connects your site to Google Search Console, which **reports on critical security issues** (like hacks or malware) that Google detects on your site.
AIOSEO	Performance & SEO	Primarily for SEO, but it helps enforce **HTTPS** and site health, which contributes to overall site trustworthiness and security signals.
WPZOOM Forms	Spam & Bot Protection	Used here specifically for its **CAPTCHA enablement** feature, which helps protect forms (contact, comments, etc.) against automated spam and bot attacks.

Recommended Resources & Further Reading

While my checklist covers the essentials, the world of security is always evolving. Use these trusted, external resources and tools to dive deeper into specific topics and maintain your site's long-term protection.

Official & Core Documentation

Resource	**Focus**	**Link**

WPBeginner Security Guide	A highly-rated, beginner-friendly guide covering common security steps in detail.	The Ultimate WordPress Security Guide – Step by Step (2025)
Let's Encrypt	Free SSL Certificates (necessary for HTTPS if your webhost doesn't provide one).	Let's Encrypt Official Site

Top-Tier Security & Auditing Tools

These tools and guides are maintained by industry experts and are highly recommended for every WordPress site.

Tool/Guide	Description & Benefit	Link
Sucuri Security Guide	A comprehensive guide to fixing and preventing malware and common attacks.	The Definitive WordPress Security Guide
UpdraftPlus Backup Plugin	A reliable solution for automated, offsite backups of your entire site (files and database).	UpdraftPlus WordPress Plugin Page

See my article **Stop Hackers: A Guide to Security** for a guide detailing the critical importance of long passwords, Multi-Factor Authentication (MFA), and the use of phishing-resistant **Passkeys**.